CONTENIDO

OBJETIVO

El presente documento pretende evidenciar detalladamente las fases del despliegue y análisis de T-pot Honeypot, una plataforma avanzada de detección de amenazas basada en contenedores.

Se abordará tanto la instalación local sobre Debian 12 como la posterior implementación en servidores de AWS. Asimismo, se analizarán los Honeypots utilizados, las configuraciones técnicas realizadas, y los indicadores de ataque detectados a través de las herramientas de análisis integradas.

FASES DEL PROYECTO

Las etapas planificadas han sido:

1. Instalación local de T-Pot y exploración inicial.
2. Selección de honeypots a implementar.
3. Configuración integral y personalización del sistema.
4. Despliegue en instancias de AWS.
5. Recolección y análisis de datos.
6. Preparación de informes técnicos y ejecutivos.
7. Cierre de pruebas y evaluación de rendimiento.

Instalación local de T-Pot y exploración inicial.

Requisitos previos

- Debian12
- Usuario con permisos sudo
- Conexión a internet estable
- Docker y Python3 instalados

Proceso de instalación

Instalamos de manera local la herramienta sobre la distribución Debian12. Para este proceso nos vamos a respaldar en el repositorio oficial https://github.com/telekom-security/tpotce (actualizado el 11.12.2024).

Creamos el usuario ordinario "amatpot" con permisos de sudo en:

```
sudo adduser amatpot
sudo usermod -aG sudo amatpot
su - amatpot
```

Desde la ubicación $HOME clonaremos el repositorio.

```
git clone https://github.com/telekom-security/tpotce
```

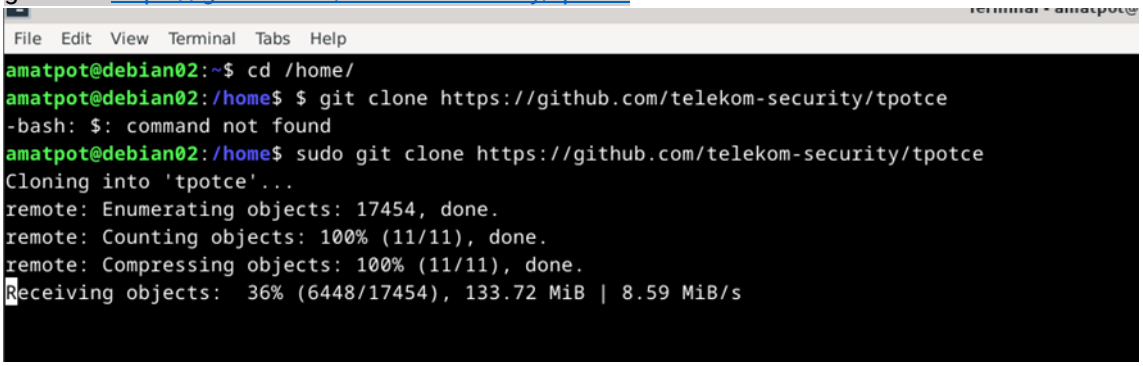


Figura 01: Clonación del repositorio de T-Pot.

Una vez clonado el repositorio, nos ubicamos en el directorio y lanzamos el instalador.

```
cd tpotce
```

```
./install.sh
```

Figura 02: Ejecución del instalador de T-Pot.

Durante la instalación seleccionaremos la opción de T-Pot Standard / HIVE installation.

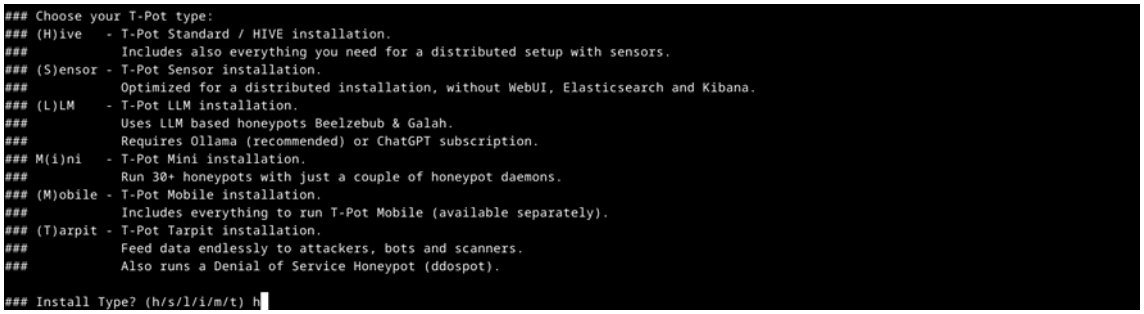


Figura 03: Opciones de tipos de T-Pot.

Para abordar las configuraciones de la herramienta, asignaremos:
user > **amatpot** y el pass > **amatpot**.

Este tipo de credenciales tienen un nivel bajo de protección ya que solo haremos un acercamiento local y en ningún momento estará expuesto a la red.

Selección de honeypots a implementar.

Ensayamos las configuraciones de los Honeypot a utilizar, nos respaldaremos en el repositorio https://github.com/telekom-security/tpotce. Haremos uso de los siguientes elementos:

Honeypots	¿Por qué los hemos elegido?
Cowrie	Simula un sistema SSH y Telnet vulnerable, registrando intentos de acceso, comandos ejecutados y técnicas de intrusión. Es útil para estudiar las tácticas, técnicas y procedimientos (TTPs).
Dionaea	Emula múltiples servicios (SMB, FTP, HTTP, etc.) para atraer malware y registrar payloads maliciosos, facilitando el análisis forense.
Conpot	Simula sistemas SCADA/ICS (Industrial Control Systems) para detectar ataques dirigidos a infraestructuras críticas, permitiendo estudiar ataques específicos contra sistemas industriales.
Elasticpot	Integra datos del honeypot en Elasticsearch para análisis avanzado y visualización en Kibana.
Honeytrap	Ofrece una plataforma flexible para crear honeypots personalizados en diferentes protocolos o servicios.
Mailoney	Detecta campañas de spam o phishing mediante la captura de correos electrónicos maliciosos o sospechosos.
WordPot	Captura intentos de explotación relacionados con vulnerabilidades en WordPress u otros CMS similares.
DDoSPot	Detecta y analizar ataques DDoS dirigidos a la infraestructura del honeypot o red protegida.
Suricata	Analiza tráfico capturado o en tránsito usando reglas específicas para identificar amenazas.
Kibana	Visualiza datos almacenados en Elasticsearch para detectar patrones o incidentes rápidamente.
Elasticsearch	Almacena grandes volúmenes de datos generados por los honeypots para facilitar búsquedas y análisis.

Configuración integral y personalización del sistema.

Para avanzar en las configuraciones de la herramienta, debemos definir el usuario WEB_USER y LS_WEB_USER en el fichero oculto ~/tpotce/.env. Desde consola creamos el user y pass, utilizamos el mismo user para ambos usuarios.

Todas las configuraciones se realizan con usuario ordinario.

```
htpasswd -n -b "amatpot" "amatpot" | base64 -w0
```

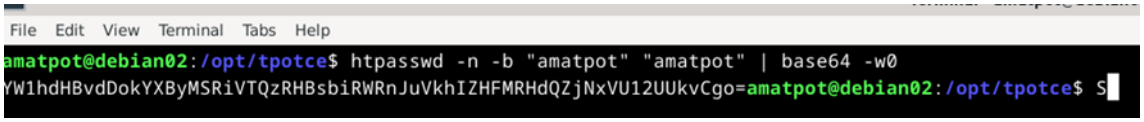


Figura 04: Creación de credenciales.

Personalización con customizer.py

Reemplazamos la información en el fichero mencionado.

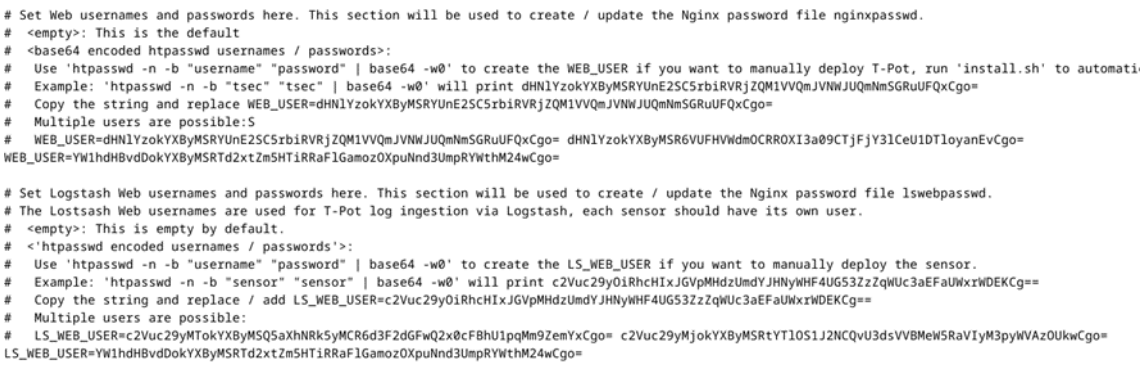


Figura 05: impactamos cambios de credenciales

Ya realizada la configuración, lanzaremos desde el directorio ~/tpotce/compose el script customizer.py.

```
sudo python3 customizer.py
```

Figura 06: ejecución del archivo customizer.py.

Copiamos el fichero personalizado en el directorio ~/tpotce.

```
sudo cp docker-compose-custom.yml ~/tpotce/
```

Figura 07: Fichero destino.

Nos movemos al directorio principal y validamos el correcto funcionamiento de la configuración realizada.

```
cd ~/tpotce/
docker compose -f docker-compose-custom.yml up
```

Figura 08: Ejecución del comando Docker compose.

Figura 09: Valoración de posibles puertos. Encabezado.

Figura 10: Levantamos h0neytr4p de docker.

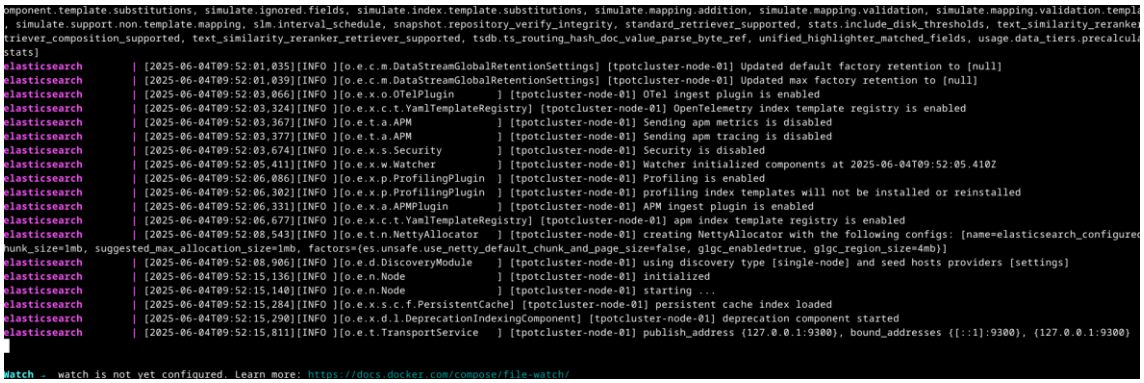


Figura 11: Levantamos Elasticsearch de docker.

Docker irá lanzando el contenedor de cada Honeypot seleccionado. Considerando que las modificaciones se realizaron de manera correcta, interrumpimos el proceso y detenemos los contenedores con el comando:

```
docker compose -f docker-compose-custom.yml down -v
```

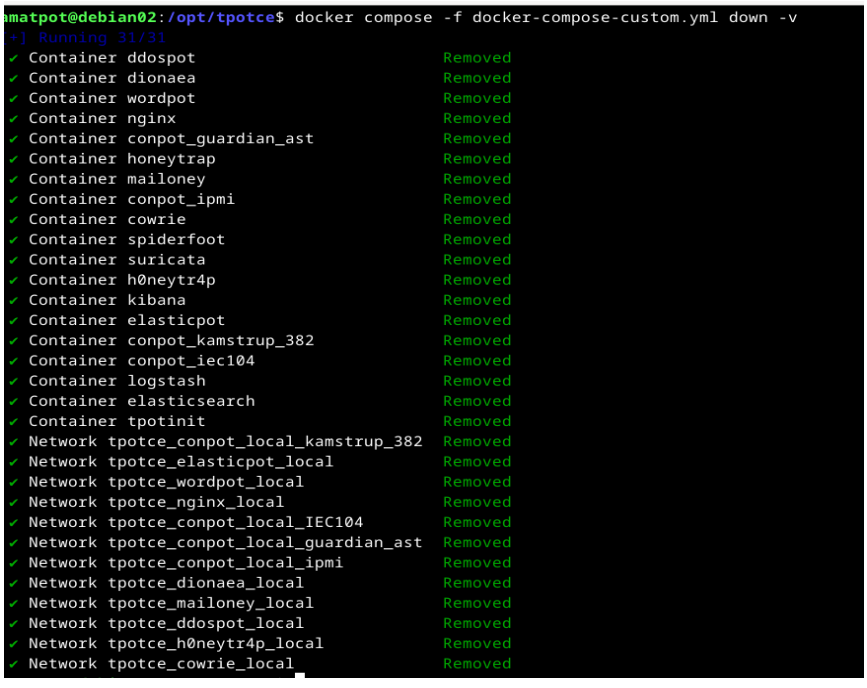


Figura 12: Lanzamiento de cada Honeypot.

En este punto reemplazamos el fichero docker-compose.yml por las configuraciones personalizadas.

```
sudo mv docker-compose-custom.yml docker-compose.yml
```

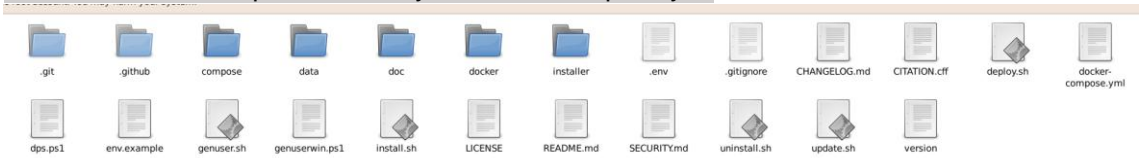


Figura 13: Reemplazamiento del archivo docker-compose.yml.

Validamos el estado actual de Tpot y lo iniciamos.

```
amatpot@debian02:/opt/tpotce$ sudo systemctl status tpot
● tpot.service - T-Pot
     Loaded: loaded (/etc/systemd/system/tpot.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-06-04 12:00:35 CEST; 36s ago
    Process: 47761 ExecStartPre=/usr/bin/docker compose -f /home/amatpot/tpotce/docker-compose.yml down -v (code=exited, status=0/SUCCESS)
   Main PID: 48097 (docker)
      Tasks: 16 (limit: 9421)
     Memory: 31.7M
        CPU: 1.644s
     CGroup: /system.slice/tpot.service
             ├─48097 /usr/bin/docker compose -f /home/amatpot/tpotce/docker-compose.yml up
             └─48111 /usr/libexec/docker/cli-plugins/docker-compose compose -f /home/amatpot/tpotce/docker-compose.yml up

Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.228348Z] Elasticsearch Honeypot by Vesselin Bontchev
Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.228391Z] Loading the plugins...
Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.229342Z] Loaded output engine: jsonlog
Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.229474Z] Listening on port 9200.
Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.229663Z] Site starting on 9200
Jun 04 12:01:12 debian02 docker[48111]: elasticpot          | [2025-06-04 10:01:12.229752Z] Starting factory <twisted.web.server.Site object at 0x7f4b198418e0>
Jun 04 12:01:12 debian02 docker[48111]: tanner_phpox        | ======== Running on http://127.0.0.1:8088 ========
Jun 04 12:01:12 debian02 docker[48111]: conpot_iec104       | /usr/lib/python3.11/site-packages/scapy/base_classes.py:324: SyntaxWarning: Packet 'SPE' has a duplicate
Jun 04 12:01:12 debian02 docker[48111]: conpot_iec104       |   warnings.warn(war_msg, SyntaxWarning)
Jun 04 12:01:12 debian02 docker[48111]: tanner_phpox        | (Press CTRL+C to quit)
lines 1-22/22 (END)
```

Figura 14: seguimiento del estado de la herramienta.

Reiniciamos el sistema para impactar las modificaciones realizadas:

```
sudo reboot
```

```
amatpot@debian02:~$ sudo systemctl status tpot
● tpot.service - T-Pot
     Loaded: loaded (/etc/systemd/system/tpot.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-06-04 12:46:14 CEST; 12s ago
    Process: 179794 ExecStartPre=/usr/bin/docker compose -f /home/amatpot/tpotce/docker-compose.yml down -v (code=exited, status=0/SUCCESS)
   Main PID: 180514 (docker)
      Tasks: 15 (limit: 9421)
     Memory: 36.7M
        CPU: 779ms
     CGroup: /system.slice/tpot.service
             ├─180514 /usr/bin/docker compose -f /home/amatpot/tpotce/docker-compose.yml up
             └─180528 /usr/libexec/docker/cli-plugins/docker-compose compose -f /home/amatpot/tpotce/docker-compose.yml up

Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |  ___) | || (_| | |  | |_| | | | | (_| |  _ _ _
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           | |____/ \__\__,_|_|_|   \__|_|_| |_|\__, | (_|_|_)
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |                                    |___/
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |  _____     ____        _       ____  _  _     ___  _  _    _
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           | |_   _|   |  _ \ ___ | |_ _  |___ \| || |   / _ \| || |  / |
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |   | |_____| |_) / _ \| __(_)   __) | || |_| | | | || |_ | |
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |   | |_____|  __/ (_) | |_ _   / __/|__   _| |_| |__   _|| |
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |   |_|     |_|   \___/ \__(_) |_____|  |_|(_)___/   |_|(_)_|
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |
Jun 04 12:46:21 debian02 docker[180528]: tpotinit           |
amatpot@debian02:~$
```

Figura 15: Comprobación de que las configuraciones funciones correctamente.

Una vez activo T-Pot, podremos visualizar los contenedores activos:

```
grc docker ps -a
```

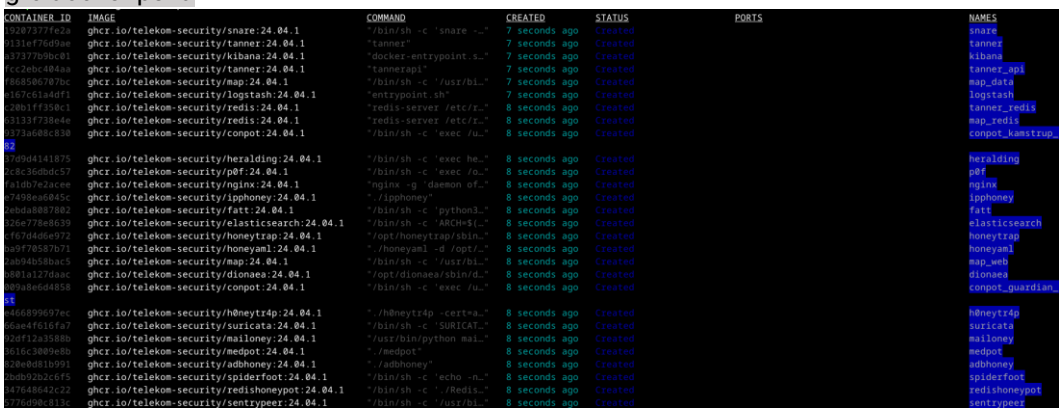


Figura 16: Contenedores activos de T-Pot.

También podremos visualizar en tiempo real, sin evidencia ya que la herramienta fue lanzada de manera local:

```
watch -c "grc --colour=on docker ps -a
```

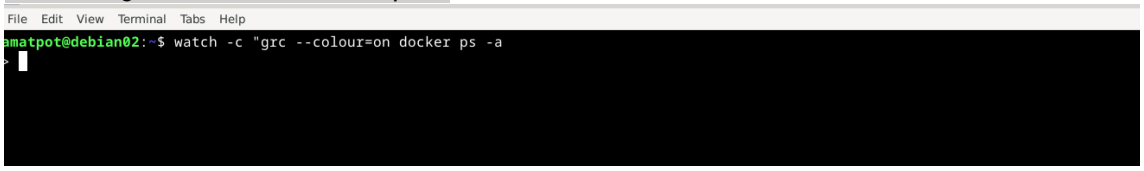


Figura 17: Monitorización en tiempo real.

Acceso vía navegador

Utilizaremos el navegador desde nuestro Host para explorar la interfaz web accediendo desde el siguiente puerto https://192.168.142.131:64297/, revisando las herramientas integradas de la plataforma:

Figura 18: Interfaz web T-Pot.

Despliegue en instancias de AWS

Para lanzar la herramienta, hemos seleccionado el servidor AWS, ya que nos permitirá configuraciones amplias de conectividad y recursos de la instancia a utilizar.

Configuraciones AWS (primer ensayo)

Abordamos las configuraciones del servidor AWS con los recursos recomendados (16GB RAM + 150GB almacenamiento)

Generamos un par de claves únicas para el acceso SSH de manera externa.

Nos conectamos al servidor con las credenciales que ofrece AWS, replicamos la instalación y configuraciones que realizamos de manera local de las herramientas y sistema. Reiniciamos Debían, y modificamos los puertos en la instancia.

64295: Para conectarnos por SSH y realizar las modificaciones y ajustes correspondientes, monitoreo de sistema.

64297: Para acceder a la interfaz web de T-Pot, revisar el Dashboard y análisis de métricas.

0-64000: Exponemos Tpot (multiples Honeypot).

ICMP: Para validar la conexión externa de la IP pública asignada.

Figura 19: Reglas de entrada en los puertos.

Configuraciones AWS (segundo ensayo)

Luego de haber realizado las configuraciones correspondientes, haber definido los Hoyneypot que lanzaremos en el primer ensayo, nos percatamos que al lanzar Tpot, la herramienta presenta intermitencias en la conexión, dejando sin utilidad la instancia. Revisando la demanda de la herramienta y la configuración vigente, decidimos modificar la cantidad de Honeypot notando un mejor rendimiento de la instancia. En este punto, también decidimos modificar los recursos del servidos y expandir RAM hasta los 32GB.

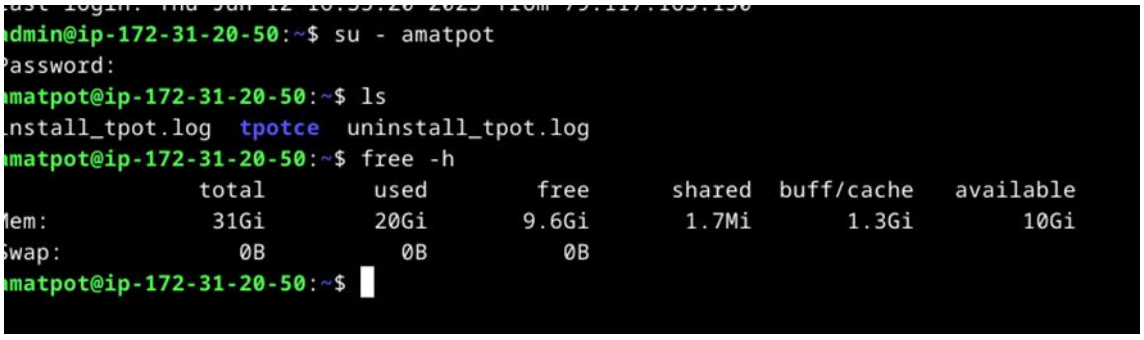


Figura 20: Capacidad de memoria usada y libre.

Con el cambio ya realizado definimos nuevamente los Honeypot a utilizar: Cowrie, Logstash, DDoSPot, Dionaea, ElasticPot, Endlessh, Heralding, Honeytrap, Mailoney, Tanner, Suricata, Elasticsearch, Kibana, Nginx Honeypot, SpiderFoot, Snare y Glutton:

Honeypots	¿Por qué los hemos elegido?
Logstash	Aunque no es un honeypot en sí, es una herramienta de procesamiento de logs que puede integrarse con honeypots para analizar eventos de seguridad.
Endlessh	Honeypot de SSH que ralentiza los ataques de fuerza bruta al enviar un banner interminable, haciendo perder tiempo a los atacantes.
Heralding	Honeypot de captura de credenciales que simula múltiples servicios como FTP, SSH, HTTP, SMTP y VNC para registrar intentos de acceso.
Tanner	Sistema de análisis que trabaja junto con Snare para evaluar solicitudes HTTP y emular vulnerabilidades en aplicaciones web.
Nginx Honeypot	Configuración de Nginx que bloquea bots maliciosos al detectar intentos de acceso a rutas sospechosas.
SpiderFoot	No es un honeypot, sino una herramienta de OSINT que recopila información sobre amenazas y posibles atacantes.
Snare	Honeypot de aplicaciones web que simula vulnerabilidades y analiza ataques dirigidos a sitios web.
Glutton	Simular servicios y vulnerabilidades relacionados con servidores web y aplicaciones web.

Recolección y análisis de datos

Análisis de T-Pot mediante Eleastic

En este apartado revisaremos la evidencia generada por la herramienta desde el 12/06 al 17/06.

Trabajamos con un sistema estable y sin cuello de botella, utilizamos solo un nodo considerando que teníamos establecido solo 6 días de evidencia.

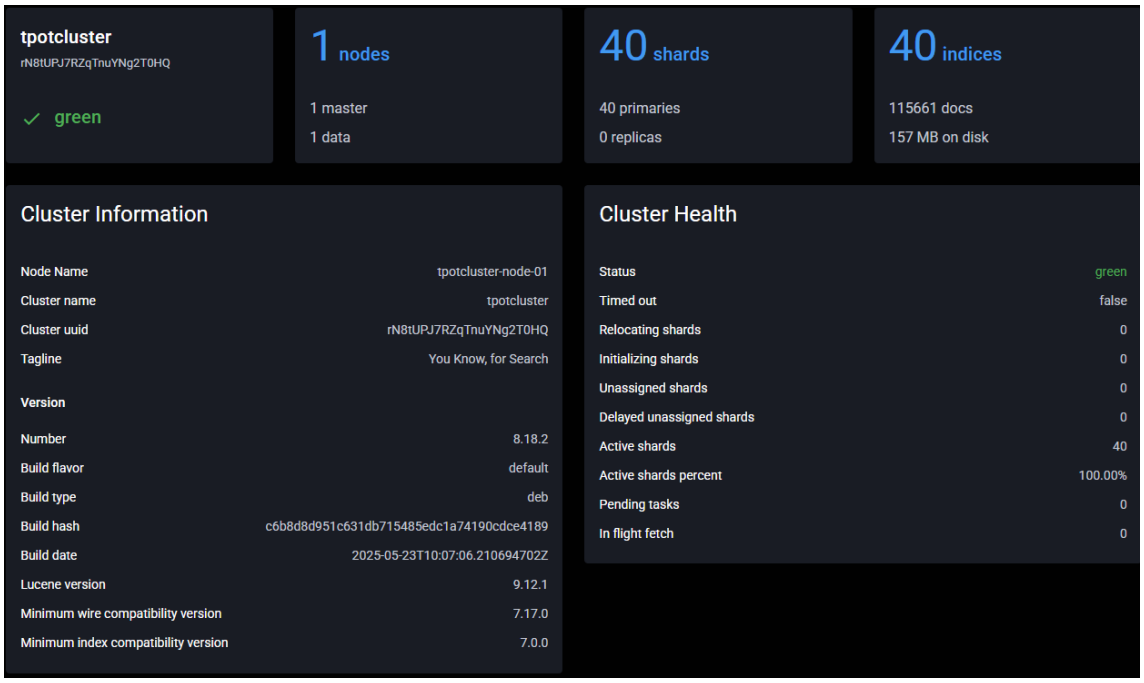


Figura 21: clúster Elasticsearch "tpotcluster"

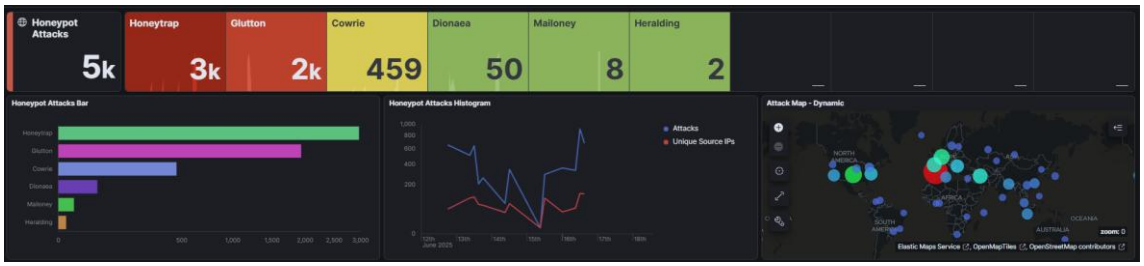


Figura 22: Vista general de Elastic sobre T-Pot.

Se han detectado un total de 5355 ataques dirigidos a los diferentes Honeypots configurados:

Honeypot	Q ataques	% Incidencia
Honeytrap	2929	54,70%
Glutton	1937	36,17%
Cowrie	429	8,01%
Dionaea	50	0,93%
Mailoney	8	0,15%
Heralding	2	0,04%
Total	5355	100,00%

Los honeypots más atacados fueron Honeytrap y Glutton, lo que sugiere que los vectores utilizados buscan explotar servicios comunes como HTTP, SSH o Telnet.

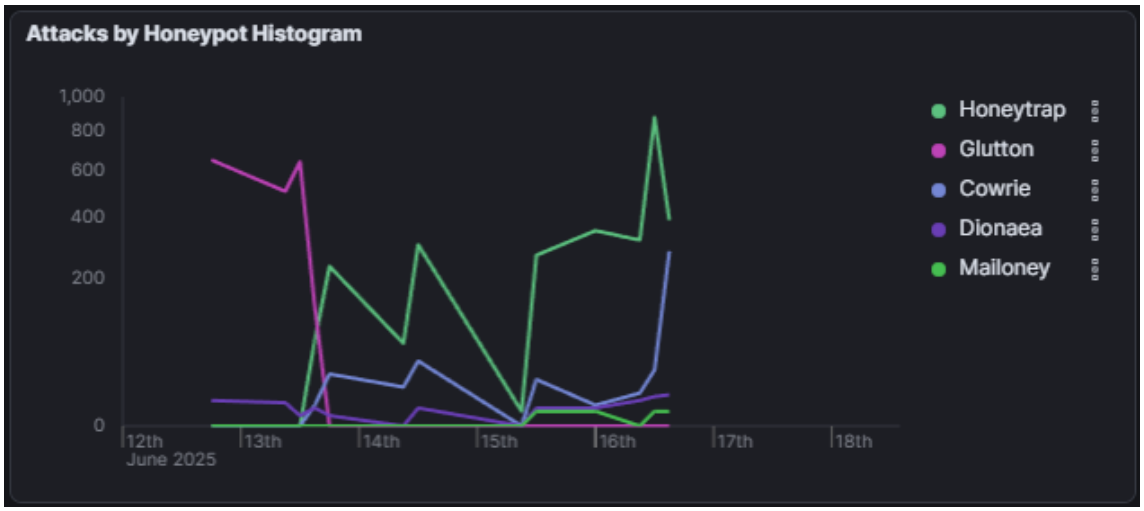


Figura 23: Gráfico que muestras diarias.

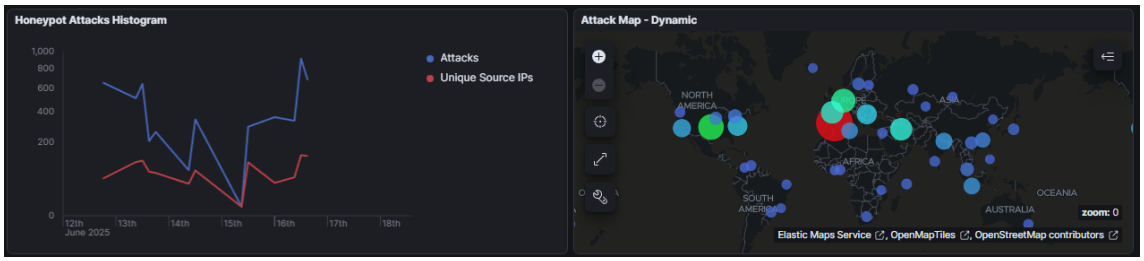


Figura 24: Histograma de ataque y mapa dinámico.

La mayoría de las IPs agresoras se concentran en:

Europa (con una concentración en Países Bajos y Alemania), Asia (China y países de Medio Oriente) y América del Norte y del Sur (actividad más dispersa, pero con especial énfasis en Estados Unidos).

En cuanto a la tendencia temporal, el histograma muestra un repunte significativo el día 16 de junio de 2025, especialmente en ataques al honeypot Honeytrap, lo que sugiere una campaña activa o un escaneo masivo coordinado.

Análisis de Cadenas de Usuario y Contraseña

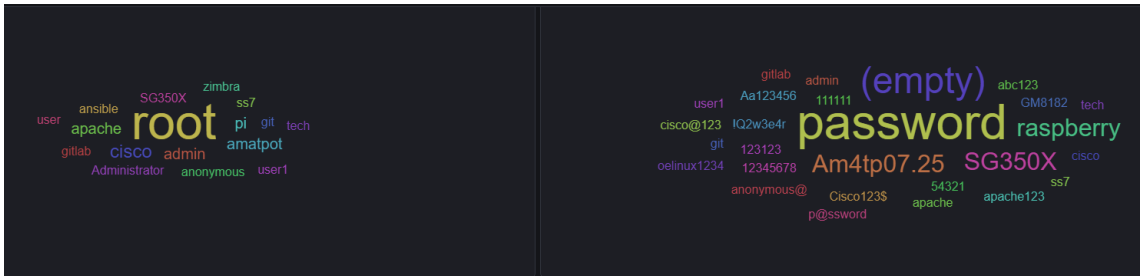


Figura 25: Nombres y contraseñas más usadas.

En los intentos de autentificación podemos observar que los nombres de usuario más usados son: root, admin, Administrator, apache, git, user o zimba entre otros. Por otro lado, las contraseñas más recurrentes son: (empty), password, 123123, Am4tp07.25, SG350X, p@ssword y raspberry.

Esto evidencia intentos de fuerza bruta simples y diccionarios básicos dirigidos a servicios expuestos.

Sistemas autónomos (AS)

Identificamos los siguientes sistemas autónomos:

AS	ASN	Count
202425	IP Volume inc	1251
14061	DIGITALOCEAN-ASN	524
63949	Akamai Connected Cloud	461
396982	GOOGLE-CLOUD-PLATFORM	260
398324	CENSYS-ARIN-01	194
55990	Huawei Cloud Service data center	177
45102	Alibaba US Technology Co., Ltd.	151
135377	UCLOUD INFORMATION TECHNOLOGY HK LIMITED	143
8075	MICROSOFT-CORP-MSN-AS-BLOCK	121
213412	ONYPHE SAS	121
63949	Linode, LLC	43
8075	Microsoft Corporation	5

Observaciones relevantes:

La mayoría de las conexiones provienen de **IP Volume Inc**. con 1,251 ocurrencias. Esta entidad es conocida por ser utilizada frecuentemente en actividades automatizadas (como escaneo masivo), y en algunos contextos puede estar asociada a tráfico potencialmente sospechoso.

Le siguen **DigitalOcean, Akamai (y Linode), y Google Cloud**, todos proveedores de servicios cloud, lo cual sugiere que el tráfico probablemente proviene de máquinas virtuales o contenedores alojados allí.

La presencia de **Censys, ONYPHE, Huawei Cloud, Alibaba, y UCLOUD** indica tráfico relacionado posiblemente con exploraciones automatizadas o actividades de reconocimiento.

Microsoft aparece dividida en dos entradas, ambas bajo ASN 8075, pero con nombres diferentes; esto puede deberse a registros distintos de base de datos o subentidades.

Principales IPs de origen malicioso:

IP	Cantidad	Observación
89.248.165.133	639	Alta actividad y reputación maliciosa.
89.248.163.83	220	Actividad constante.
1.95.78.10	168	Reputación sospechosa (Huawei Cloud).
89.248.163.57	168	Marcada como maliciosa.
89.248.163.218	114	Misma red ASN.

La IP 89.248.165.133 presenta una alta actividad y una reputación maliciosa, lo que indica un posible comportamiento dañino o sospechoso.

Otras IPs, como 89.248.163.83 y 1.95.78.10, muestran actividad constante o sospechosa, pero con menor gravedad en comparación con la primera.

La IP 89.248.163.57 está marcada como maliciosa, mientras que 89.248.163.218 pertenece a la misma red ASN, lo que sugiere que estas IPs podrían estar relacionadas o ser parte de una misma infraestructura potencialmente comprometida o utilizada para actividades maliciosas.

Vulnerabilidades conocidas CVE

La herramienta ha identificado diferentes vulnerabilidades conocidas:

CVE	Descripción	Detecciones
CVE-2021-3449	Vulnerabilidad en Pulse Connect Secure, que permite ejecución remota de código a través de una vulnerabilidad en la interfaz web.	9
CVE-2001-0540	Vulnerabilidad en Microsoft Windows relacionada con el servicio RPC (Remote Procedure Call), que puede permitir ejecución remota de código o denegación de servicio.	8
CVE-2012-0152	Vulnerabilidad en Microsoft Windows (en particular, en SMB) que puede permitir ejecución remota de código mediante un paquete SMB malicioso.	5
CVE-2019-11500	Vulnerabilidad en Apache Tomcat (versiones 8.5.x y 9.x) que permite ejecución remota de código mediante una mala configuración del servidor o explotación de ciertos endpoints.	5
CVE-2002-0013 CVE-2002-0012	Vulnerabilidades en el servidor SMTP Microsoft Exchange 5.5 que puede permitir a un atacante ejecutar comandos arbitrarios o causar denegación de servicio. Y permitiendo potencialmente ataques de escalada o ejecución remota.	2
CVE-2019-12263, CVE-2019-12261, CVE-2019-12260, CVE-2019-12255	Vulnerabilidad en sistemas Cisco ASA/Firepower que permite ejecución remota de código. Problema en Cisco Firepower Threat Defense (FTD) que puede permitir escalada de privilegios. Vulnerabilidad en Cisco ASA/FTD relacionada con la gestión y configuración. Problema similar en dispositivos Cisco relacionados con autenticación y control de acceso.	2
CVE-1999-0619	Vulnerabilidad conocida como "Ping of Death", donde paquetes ICMP malformados pueden causar fallos o reinicios en sistemas Windows y otros OS antiguos.	1
CVE-2024–6387	Este es un CVE reciente (año 2024). Sin detalles específicos disponibles aún.	1

A partir de los CVEs podemos extraer varias conclusiones:

Diversidad en los vectores de ataque:
Los CVE's abarcan diferentes tecnologías y plataformas, incluyendo sistemas operativos (Windows), servidores web (Apache Tomcat), productos de seguridad (Pulse Secure VPN o Cisco ASA), servicios de correo (Microsoft Exchange), y protocolos como SMB y ICMP. Esto refleja que las vulnerabilidades pueden afectar múltiples componentes en una infraestructura.

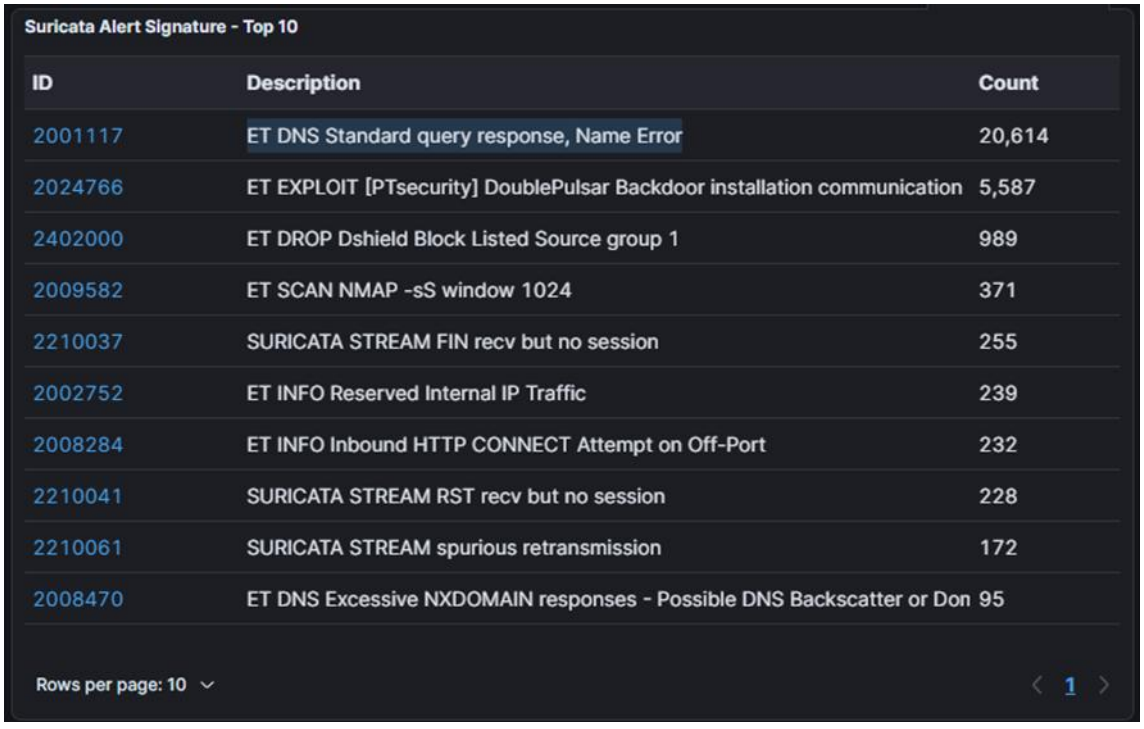
Evolución en la gravedad y sofisticación:
Algunos CVE's, como CVE-2021-3449 o CVE-2019-11500, permiten ejecución remota de código, lo cual es muy grave porque puede comprometer completamente un sistema. La presencia de vulnerabilidades recientes (2024) también indica que las amenazas evolucionan y que nuevas vulnerabilidades siguen siendo descubiertas.

Importancia de mantener los sistemas actualizados:
Muchas vulnerabilidades corresponden a versiones específicas o configuraciones incorrectas. La existencia de CVE's antiguos (como 1999 o 2001) muestra que algunos sistemas aún pueden ser vulnerables si no se actualizan o parchean adecuadamente.

Necesidad de una gestión proactiva de seguridad:
La variedad y gravedad de estos CVE's resaltan la importancia de realizar auditorías regulares, aplicar parches oportunamente, y monitorear continuamente los sistemas para detectar posibles explotaciones.

Amenazas dirigidas y automatizadas:
Algunas vulnerabilidades (como las relacionadas con servidores web o VPNs) son comúnmente explotadas por atacantes en campañas automatizadas o dirigidas para obtener acceso remoto, robar datos o lanzar ataques más complejos.

Alertas Suricata



Suricata Alert Signature - Top 10

ID	Description	Count
2001117	ET DNS Standard query response, Name Error	20,614
2024766	ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication	5,587
2402000	ET DROP Dshield Block Listed Source group 1	989
2009582	ET SCAN NMAP -sS window 1024	371
2210037	SURICATA STREAM FIN recv but no session	255
2002752	ET INFO Reserved Internal IP Traffic	239
2008284	ET INFO Inbound HTTP CONNECT Attempt on Off-Port	232
2210041	SURICATA STREAM RST recv but no session	228
2210061	SURICATA STREAM spurious retransmission	172
2008470	ET DNS Excessive NXDOMAIN responses - Possible DNS Backscatter or Don	95

Rows per page: 10 ⌄ 1

Figura 27: alertas de Suricata en T-Pot.

Detalle de las alertas críticas

ET DNS Standard query response, Name Error (20.614 eventos): Esta alerta de Suricata indica que un servidor DNS respondió que un dominio solicitado no existe, generando un código de error llamado NXDOMAIN. La alta frecuencia puede indicar actividad automatizada, como malware intentando contactar dominios inexistentes o un C2.

ET EXPLOIT [PTsecurity] DoublePulsar Backdoor installation communication (5.587 eventos): La alerta indica que se ha detectado tráfico de red asociado a la instalación del backdoor DoublePulsar, una herramienta utilizada por ciberatacantes para tomar control total de un sistema comprometido. Esta amenaza, filtrada junto con el exploit EternalBlue y relacionada con ataques masivos como WannaCry, sugiere que un dispositivo podría haber sido infectado y estar comunicándose con un atacante remoto. Es una señal clara de compromiso grave que requiere atención inmediata.

ET DROP Dshield Block Listed Source group 1 (989 eventos): Alerta o registro generado por un sistema de detección de intrusiones o un firewall que indica que un paquete de red ha sido bloqueado (DROP) porque proviene de una fuente que está en una lista de bloqueo conocida, específicamente la lista de DShield.

Nmap Scan (-sS window 1024) (371 eventos): Alerta de un escaneo rápido y sigiloso de los puertos TCP en un objetivo, enviando paquetes SYN y ajustando el tamaño de la ventana TCP a 1024 bytes. Es útil para detectar qué puertos están abiertos en un sistema sin establecer conexiones completas.

Otras alertas de interés

Tráfico desde direcciones IP internas reservadas (2002752) y conexiones HTTP a puertos no estándar (2008284) podrían indicar técnicas de evasión o configuración maliciosa en clientes comprometidos.

Alertas como RST sin sesión o retransmisiones espurias (2210041, 2210061) reflejan anomalías en el comportamiento del tráfico de red y pueden tener valor como indicadores de compromiso (IoC) cuando se correlacionan con otras señales.

Análisis Virus Total

Utilizaremos la herramienta web https://www.virustotal.com/gui/home/url para analizar las IPs más recurrentes de nuestro reporte.

Análisis 89.248.165.133

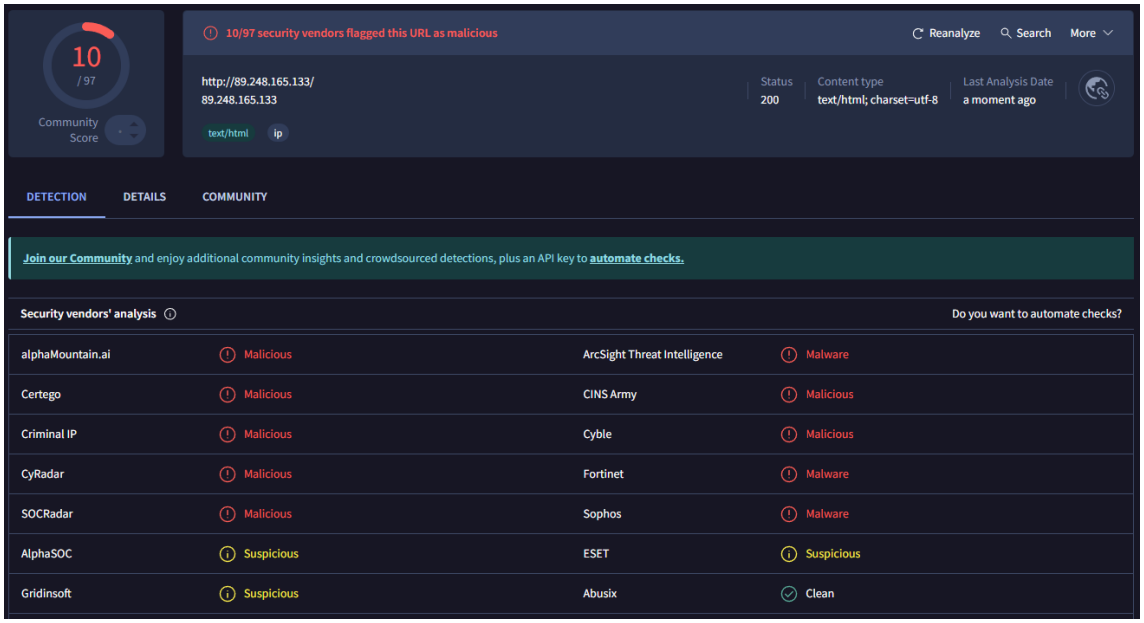


Figura 27: Análisis de la IP 89.248.165.133 en VirusTotal.

Datos generales

IP analizada	89.248.165.133
Tipo de contenido	text/html; charset=utf-8
Código de respuesta HTTP	200 OK

10 de 97 motores de seguridad clasifican la IP o URL como maliciosa.

Clasificación basada en múltiples motores de detección de amenazas, incluyendo proveedores especializados en amenazas persistentes, malware y comportamiento anómalo.

Detección de proveedores de seguridad

Clasificación	Motores de Seguridad
Malicious	alphaMountain.ai, Certego, Criminal IP, CyRadar, SOCRadar, ArcSight TI, CINS Army, Cyble, Fortinet, Sophos
Suspicious	AlphaSOC, Gridinsoft, ESET
Clean	Abusix

Riesgos potenciales identificados

La IP analizada parece estar asociada a infraestructura maliciosa, posiblemente utilizada para:

Distribución de malware.

Comando y control (C2).

Phishing o campañas automatizadas.

Recolección de información mediante técnicas ofensivas.

Esto se refuerza por la variedad y reputación de los motores de detección implicados (por ejemplo, Fortinet, Sophos, Cyble).

Implicaciones para el Entorno T-Pot

Esta IP fue capturada durante la actividad del honeypot. Tiene por significado que:

La infraestructura honeypot fue efectivamente alcanzada por actores maliciosos reales.

El tráfico capturado debe ser tratado como comprometido o de alto valor analítico.

Puede existir riesgo de exposición en caso de que la red honeypot no esté debidamente aislada.

Recomendaciones

Aislar o bloquear cualquier tráfico saliente hacia esta IP en sistemas de producción.

Revisar logs y capturas (pcap) para determinar el tipo de interacción que se intentó establecer.

Correlacionar con Suricata o Elastic Stack para visualizar el contexto completo del ataque (hora, protocolo, CVE explotado, etc.).

Considerar esta IP como parte de una lista negra interna para futuras detecciones.

Notificar al equipo de respuesta ante incidentes (CSIRT) en caso de que haya indicios de contacto fuera del entorno honeypot.

Análisis 1.95.78.10

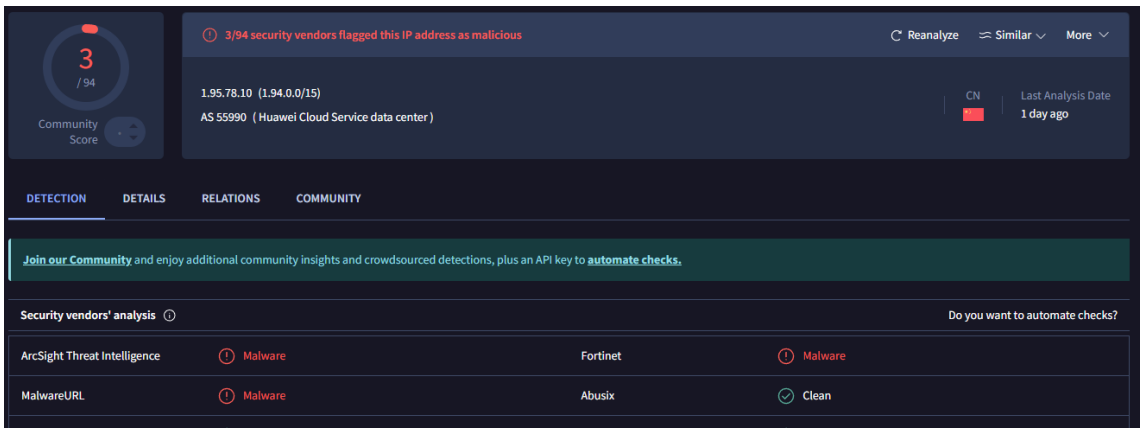


Figura 28: Análisis de la IP 1.95.78.10 en VirusTotal.

Datos generales

IP Analizada	1.95.78.10
Rango CIDR	1.94.0.0/15
Proveedor de red (ASN)	AS 55990 – Huawei Cloud Service Data Center
Ubicación	China (CN)

3 de 94 motores de seguridad clasifican esta IP como maliciosa.

Aunque el número total de motores es alto, la proporción de detección es baja. Esto sugiere un riesgo moderado o una posible falsa alarma, pero requiere atención debido al contexto de uso en honeypots o análisis de amenazas.

Detección de proveedores de seguridad

Clasificación	Motores de Seguridad
Malicious/Malware	ArcSight Threat Intelligence, MalwareURL, Fortinet
Clean	Abusix

Riesgos potenciales identificados

Proveedor de red: Huawei Cloud

Esta IP pertenece a un rango de direcciones de un proveedor de nube.

Implicación: Puede tratarse de infraestructura alquilada por actores legítimos o maliciosos, lo que es común en campañas temporales o botnets.

Geolocalización: China

En análisis de inteligencia de amenazas, la procedencia geográfica puede ser un factor adicional, ya que algunos entornos restringen comunicaciones con ciertos países por razones de ciberseguridad.

Implicaciones para el Entorno T-Pot

Esta IP fue registrada en los logs de un honeypot:

Es probable que haya participado en actividades de reconocimiento o ataque automatizado.

La detección por múltiples motores aumenta su valor como IOC (Indicador de Compromiso).

Debe correlacionarse con el tipo de tráfico (por ejemplo, escaneos, intentos de login, uso de exploits).

Recomendaciones

Registrar esta IP en listas internas de vigilancia (blacklist temporal o lista de observación).

Correlacionar eventos con registros de Suricata, Cowrie o Dionaea para conocer el tipo de actividad recibida.

Si el tráfico fue significativo o recurrente, analizar capturas pcap asociadas a la conexión.

Utilizar herramientas OSINT (Shodan, AbuseIPDB) para comprobar actividad histórica.

Análisis 89.248.163.57

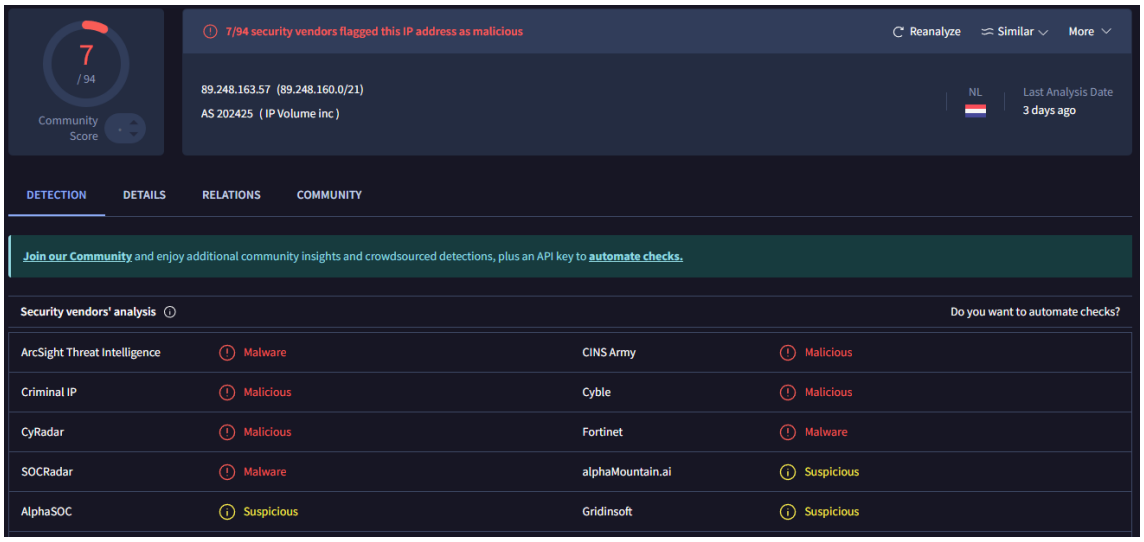


Figura 28: Análisis de la IP 1.95.78.10 en VirusTotal.

Datos generales

IP Analizada	89.248.163.57
Rango CIDR	89.248.160.0/21
Proveedor de red (ASN)	AS202425 – IP Volume Inc.
Ubicación	Países Bajos (NL)

7 de 94 motores de seguridad clasifican esta IP como maliciosa.

Este número, aunque no representa mayoría, es significativo para considerar esta IP como una amenaza potencial, especialmente en entornos sensibles o expuestos a internet.

El contexto sugiere uso asociado a infraestructura sospechosa o directamente hostil.

Detección de proveedores de seguridad

Clasificación	Motores de Seguridad
Malicious/Malware	ArcSight Threat Intelligence, Criminal IP, CyRadar, SOCRadar, CINS Army, Cyble y Fortinet
Suspicious	alphaMountain.ai, AlphaSOC y Gridinsoft

Riesgos potenciales identificados

Proveedor de Red – IP Volume Inc.

Esta organización ha sido asociada en diversas bases OSINT a alojamientos utilizados para campañas de spam, malware o comportamientos automatizados.

Las IPs bajo su gestión a menudo son utilizadas como nodos temporales en botnets o servidores de comando y control (C2).

Ubicación: Países Bajos

Si bien los Países Bajos son una jurisdicción avanzada en términos tecnológicos, su infraestructura cloud es a veces utilizada por actores maliciosos por su accesibilidad.

Implicaciones para el Entorno T-Pot

La IP fue capturada por el entorno T-Pot, se pueden extraer las siguientes conclusiones:

Interacción maliciosa real: El honeypot ha recibido tráfico de una IP señalada por múltiples motores de seguridad.

Valor como IOC (Indicador de Compromiso): La IP puede ser registrada y utilizada en reglas de detección, listas negras y retroanálisis de tráfico.

Oportunidad de análisis forense: Se sugiere investigar los logs y paquetes asociados a la conexión desde esta IP para identificar intentos de explotación, comandos o payloads.

Recomendaciones

Bloquear o monitorear esta IP en redes corporativas o críticas.

Cruzar datos con otras fuentes como AbuseIPDB, Shodan o AlienVault OTX.

Evaluar la interacción registrada en el honeypot: protocolo utilizado, puertos, CVEs asociados.

Mantener esta IP como referencia en sistemas de detección temprana y protección perimetral.

Escaneo mediante SpiderFoot

Resumen general del escaneo

Se escaneó un total de 623 elementos, de los cuales han sido identificados 448.

El análisis se ha completado con éxito, sin errores. Se identificaron 10 correlaciones relevantes, de las cuales 5 representan un riesgo alto.

Altas: 5

Medias: 0

Bajas: 0

Informativas: 5

Distribución de Tipos de Datos Analizados

El gráfico muestra una predominancia de Web Content – URLs con un 22%, Affiliate – IP Address con un 20%, Web Content – SHA256 con un 14% y Phone Number con un 7%.

Esto indica una fuerte actividad relacionada con las infraestructuras sospechosas (IPs afiliadas), recolección de contenido web malicioso (URLs y hashes) y un posible involucramiento de campañas fraudulentas vía telefonía.

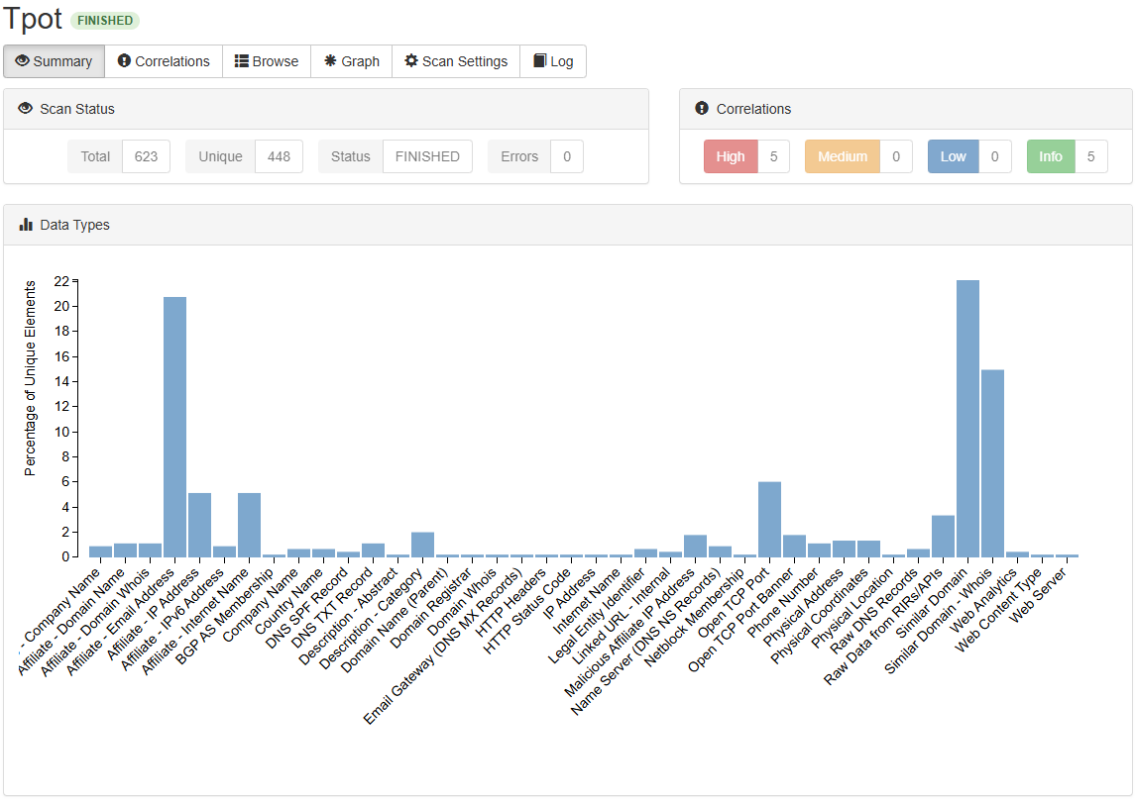


Figura 29: Grafico de SpiderFoot.

Correlaciones Detectadas

Se detectaron varias exposiciones de servicios y configuraciones que representan vulnerabilidades críticas. Las representaremos en esta tabla:

Tipo de correlación	Riesgo	IP/Elemento afectado	Detalles
Exposición de base de datos	Alto	56.228.5.102:1521	Oracle DB (Puerto 1521)
Exposición de base de datos	Alto	56.228.5.102:3306	MySQL (Puerto 3306)
Exposición de base de datos	Alto	56.228.5.102:5432	PostgreSQL (Puerto 5432)
Exposición de base de datos	Alto	56.228.5.102:9000	Servicio personalizado/inseguro.
Exposición de escritorio remoto	Alto	56.228.5.102	Riesgo de acceso no autorizado.
Outlier geográfico	Info	Suecia	Localización inusual o sospechosa.
Software revelado en puertos	Info	SSH/OpenSSH y VNC (RFB 003.007)	Posible fingerprinting del sistema.

Tpot FINISHED

Summary | Correlations | Browse | Graph | Scan Settings | Log

Correlation	Risk	Data Elements
Base URL requires authentication: ec2-56-228-5-102.eu-north-1.compute.amazonaws.com	INFO	1
Database server exposed to the Internet: 56.228.5.102:1521	HIGH	1
Database server exposed to the Internet: 56.228.5.102:3306	HIGH	1
Database server exposed to the Internet: 56.228.5.102:5432	HIGH	1
Database server exposed to the Internet: 56.228.5.102:9000	HIGH	1
Outlier country found: Sweden	INFO	1
Remote desktop exposed to the Internet: 56.228.5.102	HIGH	2
Software version revealed on open port: 4	INFO	1
Software version revealed on open port: RFB 003.007	INFO	1
Software version revealed on open port: SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10	INFO	1

Figura 30: Correlaciones detectadas en SpiderFoot.

Tpot FINISHED

Summary | Correlations | Browse | Graph | Scan Settings | Log

Correlation	Risk	Data Elements
Base URL requires authentication: ec2-56-228-5-102.eu-north-1.compute.amazonaws.com	INFO	1
Database server exposed to the Internet: 56.228.5.102:1521	HIGH	1

Data Element	Source Data Element	Source Module	Identified
56.228.5.102:1521	56.228.5.102	sfp_portscan_tcp	2025-06-16 09:45:24

Database server exposed to the Internet: 56.228.5.102:3306	HIGH	1

Data Element	Source Data Element	Source Module	Identified
56.228.5.102:3306	56.228.5.102	sfp_portscan_tcp	2025-06-16 09:46:25

Database server exposed to the Internet: 56.228.5.102:5432	HIGH	1

Data Element	Source Data Element	Source Module	Identified
56.228.5.102:5432	56.228.5.102	sfp_portscan_tcp	2025-06-16 09:45:24

Database server exposed to the Internet: 56.228.5.102:9000	HIGH	1

Data Element	Source Data Element	Source Module	Identified
56.228.5.102:9000	56.228.5.102	sfp_portscan_tcp	2025-06-16 09:44:24

Outlier country found: Sweden	INFO	1
Remote desktop exposed to the Internet: 56.228.5.102	HIGH	2

Figura 31: Correlaciones críticas desplegadas.

Visualización de Red de Relaciones

La vista del grafíco muestra un entorno altamente interconectado, con cientos de nodos y relaciones entre elementos. Destaca un nodo (en rojo) que representa un elemento de alto riesgo, probablemente uno de los expuestos a Internet con múltiples conexiones. Este nodo puede estar actuando como centro de infraestructura maliciosa, permitiendo pivotar hacia otras entidades.

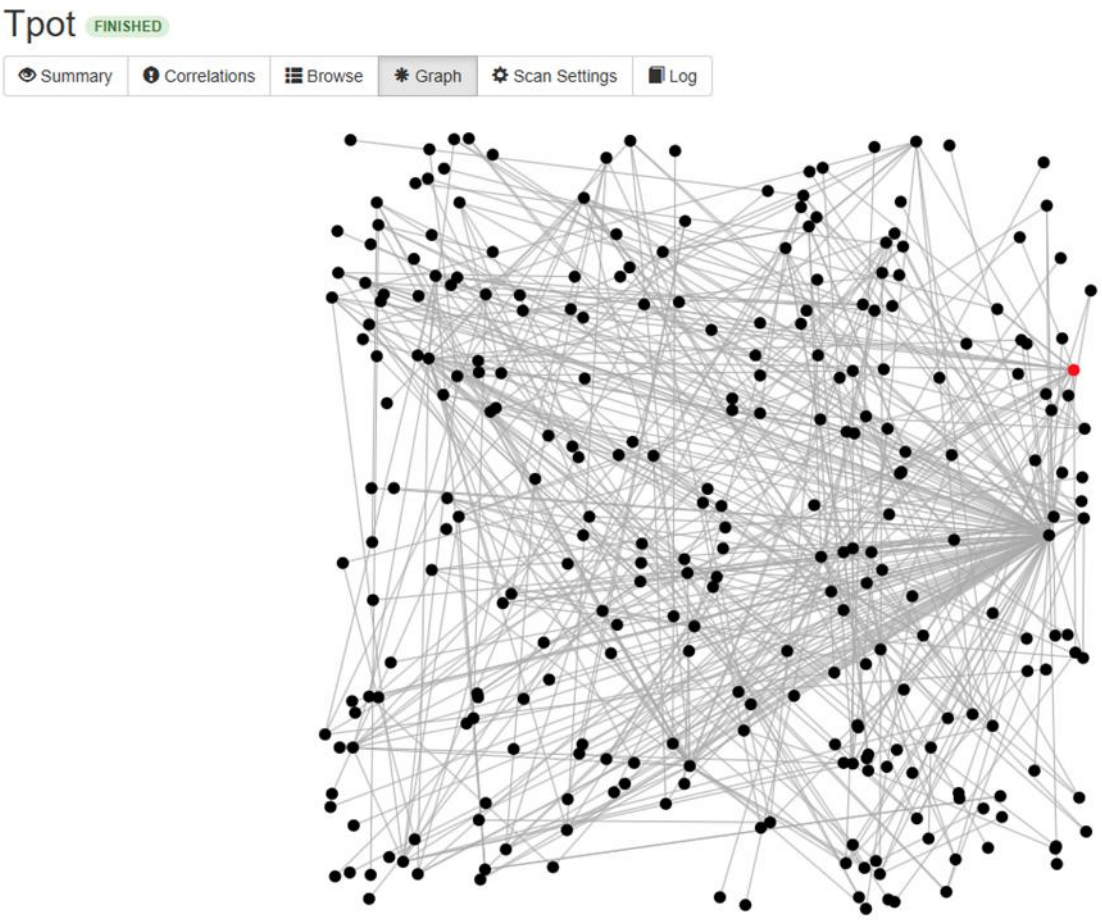


Figura 32: Gráfico de nodos.

Evaluación de Riesgos

Podemos agrupar estos elementos de riesgo en 4.

Exposición directa de bases de datos a Internet: permite ataques de enumeración, inyección SQL, acceso no autenticado, etc.

Servicios identificables por fingerprinting: expone detalles del sistema operativo o versiones, facilitando ataques dirigidos.

Presencia de escritorio remoto abierto: riesgo de ransomware o compromisos directos.

Ubicación anómala (Suecia): si no se corresponde con la infraestructura habitual, puede indicar uso de servicios de anonimato (VPN, proxies, cloud externo).

Recomendaciones

Cierre inmediato o restricción de puertos abiertos: Limitar acceso a servicios como Oracle, MySQL, PostgreSQL solo desde IPs autorizadas.

Aplicar firewalls y reglas de segmentación de red: para proteger servicios internos no destinados al acceso público.

Revisión de accesos remotos: desactivar RDP si no es esencial y aplicar MFA.

Ocultar software y versiones expuestas: aplicar técnicas de obfuscación, headers neutros y deshabilitar banners.

Monitoreo de tráfico saliente/interno con anomalías geográficas.

Análisis mediante VirusTotal

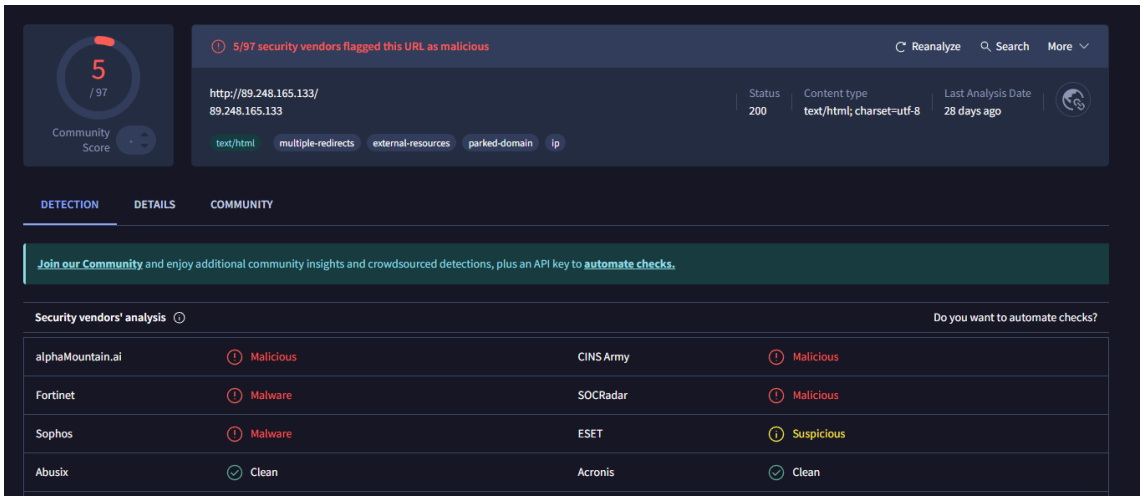


Figura 33: Analisis de VirusTotal sobre la IP 89.248.165.133.

Datos generales

Dirección IP analizada	http://89.248.165.133/
Tipo de contenido	text/html; charset=utf-8
Código de respuesta	200 OK (sitio accesible)
Último análisis	Hace 28 días
Etiquetas asociadas	text/html, multiple-redirects, external-resources, parked-domain, ip

Detección de proveedores de seguridad

De un total de 97 motores de análisis, 5 lo han marcado como malicioso.

Proveedor	Clasificación
alphaMountain.ai	Malicious
Fortinet	Malicious
Sophos	Malicious
CINS Army	Malicious
SOCRadar	Malicious
ESET	Suspicious

Abusix / Acronis	Clean

Resultado: 5/97 motores de detección han identificado esta IP como maliciosa, lo cual sugiere una actividad potencialmente dañina, aunque no categóricamente confirmada por el consenso general.

Características técnicas del Dominio/IP

Redireccionamientos múltiples: Posible camuflaje o técnica evasiva para ocultar el destino final de una carga maliciosa.

Recursos externos: Podría vincularse con servicios externos para cargar scripts, trackeo o ejecutar cargas útiles.

Dominio estacionado (parked-domain): Es posible que la IP se relacione con un dominio inactivo usado para fines de phishing, entrega de malware o campañas maliciosas temporales.

Riesgos potenciales identificados

Distribución de malware: Al menos dos motores lo han clasificado como malware host.

Comportamiento evasivo (redirects y recursos externos): Indicios de manipulación del tráfico o encubrimiento de intenciones reales.

Dominio sin actividad legítima aparente: Puede estar esperando ser utilizado o servir como nodo de rebote.

Recomendaciones

Bloqueo preventivo: Restringir acceso desde y hacia esta IP en los sistemas de red y endpoints.

Monitoreo activo: Verificar logs internos en busca de comunicaciones previas o actuales con esta dirección IP.

Análisis forense: Si se detecta interacción, analizar paquetes de red o archivos descargados para determinar si hubo ejecución de código malicioso.

Análisis periódicos: Considerar la evolución del comportamiento asociado a esta IP realizando reanálisis regulares.

Revisión VirusTotal

Automatizamos la consulta utilizando Script (vt_ip_lookup.py) y API keys de Virus Total, obteniendo los siguientes resultados y conclusiones:

IP	Maliciosos	Sospechosos	Ultimo Análisis	Pais	ASN	ISP
89.248.165.133	11	3	16/06/2025 16:59	Países Bajos	202425	IP Volume inc
89.248.163.83	11	3	01/06/2025 0:15	Países Bajos	202425	IP Volume inc
1.95.78.10	4	0	15/06/2025 13:00	China	55990	Huawei Cloud Service data center
89.248.163.57	7	3	13/06/2025 1:23	Países Bajos	202425	IP Volume inc
89.248.163.218	14	1	03/06/2025 23:03	Países Bajos	202425	IP Volume inc
143.110.142.48	7	4	06/06/2025 13:51	Estados Unidos	14061	DIGITALOCEAN-ASN
149.40.50.205	4	1	13/06/2025 17:55	Estados Unidos	212238	Datacamp Limited
146.70.212.85	1	0	07/02/2025 12:42	Estados Unidos	9009	M247 Europe SRL
185.91.127.81	11	2	18/06/2025 11:06	Alemania	49581	Tube-Hosting
134.122.78.78	6	3	17/06/2025 0:20	Alemania	14061	DIGITALOCEAN-ASN

IPs con alta detección maliciosa

Estas direcciones tienen más de 10 detecciones maliciosas, lo que indica una presencia consistente en listas negras:

89.248.165.133 – 11 maliciosos / 3 sospechosos / País: NL / ASN: 202425 (IP Volume Inc.)

89.248.163.83 – 11 / 3 / NL / IP Volume

89.248.163.218 – 14 / 1 / NL / IP Volume

185.91.127.81 – 11 / 2 / DE / Tube-Hosting

Observación: IP Volume Inc. aparece reiteradamente. Este proveedor es conocido por su infraestructura alquilada para escaneo automatizado y, en muchos casos, uso malintencionado (bots, probing, etc.). Estas IPs deberían considerarse para bloqueo o cuarentena, especialmente en entornos expuestos públicamente.

IPs con actividad intermedia o potencialmente agresiva

89.248.163.57 – 7 / 3 / NL / IP Volume Inc.

143.110.142.48 – 7 / 4 / US / DigitalOcean

134.122.78.78 – 6 / 3 / DE / DigitalOcean

Nota: Aunque los valores están por debajo de 10, son lo suficientemente altos como para indicar que han sido asociadas con actividad sospechosa. Vale la pena monitorearlas o establecer reglas de firewall condicionales.

IPs con baja detección pero relevantes.

1.95.78.10 – 4 / 0 / CN / Huawei Cloud

149.40.50.205 – 4 / 1 / US / Datacamp Limited

146.70.212.85 – 1 / 0 / US / M247 Europe

Estas pueden usarse como nodos de evasión (VPNs, proxies o entornos cloud públicos). Aunque la actividad reportada es más baja, conviene contextualizar con logs propios para saber si vale la pena bloquearlas.

Recomendaciones generales

IP Volume Inc. debería ser considerada una fuente de riesgo alto en esta muestra.

Revisa si alguna de estas IPs ha interactuado con servicios sensibles o internos. Si es así, procede al aislamiento o reporte.

Si el entorno es de producción, puedes automatizar el bloqueo de cualquier IP con más de X detecciones maliciosas.

Usar herramientas como fail2ban, iptables, o integración con sistemas SIEM puede ayudarte a mitigar automáticamente.

Revisión Análisis AbuseIPDB

Automatizamos la consulta en la plataforma AbuseIPDB con Script (abuseipdb_lookup.py) y API keys, valorando los siguientes reportes comunitarios y conclusiones:

IP	Abuse Score	Total Reportes	Pais	Dominio	ISP	Hostname
89.248.165.133	100	155	Países Bajos	recyber.net	RECYBER PROJECT NETBLOCK	recyber.net
89.248.163.83	100	127	Países Bajos	recyber.net	RECYBER PROJECT NETBLOCK	N/A
1.95.78.10	100	28	China	drpeng.com.cn	Beijing Teletron Telecom Engineering Co., Ltd.	ecs-1-95-78-10.compute.hwclouds-dns.com
89.248.163.57	100	122	Países Bajos	recyber.net	RECYBER PROJECT NETBLOCK	N/A
89.248.163.218	100	97	Países Bajos	recyber.net	RECYBER PROJECT NETBLOCK	recyber.net
143.110.142.48	100	680	Estados Unidos	digitalocean.com	DigitalOcean, LLC	prod-beryllium-sfo2-31.do.binaryedge.ninja
149.40.50.205	66	35	Estados Unidos	datacamp.co.uk	Datacamp Limited	unn-149-40-50-205.datapacket.com
146.70.212.85	38	41	Estados Unidos	m247.com	M247 New Jersey Infrastructure	N/A
185.91.127.81	100	24705	Alemania	tube-hosting.com	Ferdinand Zink trading as Tube-Hosting	tube-hosting.com
134.122.78.78	100	134	Alemania	digitalocean.com	DigitalOcean, LLC	N/A

IPs altamente peligrosas (Abuse Score 100)

Estas IPs recibieron el máximo puntaje de abuso, lo que indica que han sido reportadas consistentemente por múltiples fuentes por comportamiento malicioso (por ejemplo: escaneo de puertos, intentos de intrusión, spam, DDoS):

89.248.165.133 / 89.248.163.83 / 89.248.163.57 / 89.248.163.218 Todas de recyber.net bajo RECYBER PROJECT NETBLOCK (Países Bajos). Están alojadas en infraestructura de hosting y han sido reportadas decenas de veces solo en los últimos días. Usualmente asociadas a campañas automatizadas de escaneo o scraping agresivo.

1.95.78.10 Servidor chino (Huawei cloud), también con 100 de score. Su hostname sugiere un entorno cloud. Aunque con menor cantidad de reportes (28), haber alcanzado 100 indica que esos reportes fueron recientes y confiables.

143.110.142.48 DigitalOcean, Estados Unidos, con 680 reportes, lo que la hace extremadamente sospechosa. Además, su hostname sugiere monitoreo por parte de BinaryEdge, lo cual refuerza la sospecha de escaneo activo.

185.91.127.81 Esta IP alemana aparece como crítica: ¡más de 24.700 reportes! Posiblemente parte de campañas automatizadas o infraestructura comprometida. Perteneciente a Tube-Hosting, debe ser tratada como una amenaza directa.

134.122.78.78 Otra instancia de DigitalOcean en Alemania. Puntaje máximo también, aunque sin hostname visible. Claramente figura como actor no confiable.

IPs con riesgo moderado

149.40.50.205 Score de 66 sobre 100. Ubicada en Datacamp, muy probablemente relacionada con proxies/VPNs o servicios que pueden ser mal utilizados. Tiene hostname asignado, lo que sugiere que está en producción, pero ha sido reportada varias veces.

IP con bajo riesgo relativo

146.70.212.85 Puntaje 38, lo que indica una actividad dudosa pero no concluyentemente maliciosa. M247 es conocida por alquilar infraestructura para VPNs y puede ser usada para evasión o testing legítimo. De todas formas, con 41 reportes, conviene monitorearla.

CONCLUSIONES

El desarrollo de este proyecto ha permitido desplegar con éxito un entorno completo de honeypots mediante la plataforma T-Pot, tanto en entornos locales como en servidores Cloud (AWS), logrando capturar, analizar y evaluar una amplia variedad de amenazas reales en tiempo real.

Se ha demostrado la capacidad de T-Pot para integrar múltiples honeypots de manera eficiente, así como herramientas complementarias como Suricata, Elasticsearch y Kibana, que han facilitado el análisis avanzado de incidentes y la visualización de patrones de ataque.

Entre los resultados más relevantes, destacan:

Más de 5.000 ataques registrados, siendo Honeytrap y Glutton los honeypots más atacados.

Identificación de múltiples IPs maliciosas, como 89.248.165.133, con alta actividad y reputación negativa en bases OSINT.

Detección de intentos de acceso con credenciales comunes o vacías, confirmando la persistencia de ataques de fuerza bruta automatizados.

Presencia de ataques relacionados con vulnerabilidades críticas (CVE), como DoublePulsar, Apache Tomcat o servicios de VPN y correo.

Evidencia de infraestructura maliciosa global: ataques originados principalmente desde Europa, Asia y Norteamérica, algunos provenientes de proveedores cloud (Huawei, IP Volume Inc.).

Asimismo, el uso de herramientas como SpiderFoot y VirusTotal ha permitido enriquecer el análisis con datos externos, correlacionando actividad de red con indicadores de compromiso conocidos (IoCs).

La experiencia ha servido no solo para validar la efectividad de T-Pot como plataforma de ciberinteligencia, sino también para entender el comportamiento real de actores maliciosos y fortalecer estrategias de detección, contención y respuesta.

En resumen, el proyecto ha cumplido satisfactoriamente sus objetivos técnicos, formativos y operativos, sentando las bases para futuras investigaciones en ciberseguridad defensiva y análisis de amenazas.